



Cloud Computing Specialist CERT/CCS

Cloud Security Kurs für Informationssicherheitsbeauftragte, Risikomanager und Cloud-Architekten. Im ersten Teil werden Cloud-Grundlagen behandelt und wichtige Begriffe definiert. Im zweiten Teil werden Basistechnologien der Cloud wie Compute, Network und Storage verständlich erläutert. Governance, Risk, Compliance (GRC), also Risiken und Gefährdungen der Cloud u.a. für das Unternehmen und den Datenschutz bilden den dritten Teil. Maßnahmen zur Absicherung der Cloud, Penetrationstests und Forensik von Cloud-Diensten sind Bestandteile des vierten Teils. Im letzten Teil des Seminars werden die Cloud-Angebote der führenden Hyperscaler detailliert betrachtet und die angebotenen Sicherheitsmaßnahmen bewertet.

Unser Experten-Zertifikat ermöglicht es Ihnen als Mitarbeiter Ihre Kompetenz im Umfeld Informationssicherheit eindeutig zu belegen.

Listenpreis

3.390,00 € exkl. MwSt

4.034,10 € inkl. MwSt

Dauer

5 Tage

Gebühr für Prüfungen/Examen

390,00 € exkl. MwSt / 464,10 € inkl. MwSt

Prüfungsversicherung

159,00 € exkl. MwSt / 189,21 € inkl. MwSt

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin



Manuela Krämer

Leitung
Informationssicherheit

Kontakt/Fragen:

m.kraemer@cbt-training.de

Telefon: +49 (0)89-4576918-12

Inhalte

1. Tag

- **Warum Cloud Services?**
 - Chance in der Cloud
- **Cloud-Definition der NIST**
 - NIST SP 800-145
 - Allgemein über das Internet erreichbar
 - On-Demand Selbstservice
 - Hohe Elastizität der Ressourcen
 - Messbarkeit der Nutzung
 - Verteilte Systeme (Ressourcen Pool)
- **Cloud Referenzarchitektur**
 - ISO 17789
 - ENISA
- **Verantwortlichkeiten**
 - Cloud Provider
 - Cloud User/Consumer
 - Cloud Broker
 - Cloud Auditor
- **Cloud Varianten**
 - Infrastruktur-as-a-Service (IaaS)



- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)
- Sonstige z.B. Security-as-a-Service (SECaaS)
- **Öffentliche, private und hybride Cloud-Modell**

2. Tag

- **Basisbausteine**
 - Compute
 - Virtual CPUs/Cores
 - Network
 - Overlay Networks
 - Storage Networks
 - Storage
 - Object Storage
 - Volume Storage
 - Database Storage
- **Virtualisierung**
 - Hypervisor
- **Container**
 - Docker
 - Kubernetes
- **Entwicklungsprozesse in der Cloud**
 - Continuous Integration/Continuous Delivery (CI/CD)
 - Infrastructure as Code (IaC)
- **Serverless Computing**

3. Tag

- **Informationssicherheit in der Cloud**
 - CSK Security Guidance v4
- **Risiken von Cloud-Diensten**
 - ENISA Cloud Computing Security Risk Assessment
 - Compliance, Recht, Datenschutz
 - Verfügbarkeit
 - Vendor Lock-In
 - Governance
- **Verschlüsselung**
 - Storage Encryption
 - Transport Encryption
 - Key Management
- **Identitätsmanagement**
 - Multifaktor-Authentisierung
 - Risk-based Authentication
- **Penetrationstests von Cloud-Diensten**
- **Forensische Analyse in Cloud-Diensten**
 - Logfiles
 - Vorgehensweise

4. Tag

- **IT-Service-Management in Cloud-Umgebungen**
 - Hybrides Management
 - Lizenzierung
 - IT-Operation
 - Cloud-Migration
 - Automatisierung



- Self-Service Portale
- Service Level Agreements
- KPI in Cloud-Umgebungen
 - Relevante Leistungsindikatoren
 - Messmittel und Messwerte
- **Microsoft Azure**
 - Einführung in Microsoft Azure
 - Azure Virtual Machines
 - Azure Container Instances
 - Azure Kubernetes Service
 - Windows Virtual Desktop
 - Azure-Speicherdienste
 - Azure Blob Storage
 - Azure Disk Storage
 - Azure File Storage
 - Azure Sicherheit
 - Azure AD Identity Protection (Cloud only)
 - Azure AD (Authentifizierung)
 - Azure Information Protection und Windows Information Protection
 - Microsoft 365
 - Office, AD, Cloud-Integration

5. Tag

- **Amazon AWS**
 - Einführung in Amazon Web Services
 - Nutzungsbasiertes Preismodell
 - AWS Well-Architected Framework
 - Vorteile von Cloud Computing
 - Amazon Elastic Compute Cloud (Amazon EC2)
 - Grundkonzept von Availability Zones
 - Öffentliche und private Netzwerkkressourcen
 - Amazon Storage
 - Amazon Elastic Block Store (Amazon EBS)
 - Amazon Simple Storage Service (Amazon S3)
 - Amazon Elastic File System (Amazon EFS)
 - Amazon Relational Database Service (Amazon RDS)
 - Sicherheitsfunktionen
 - Grundlegende Sicherheitsrichtlinien
 - AWS Identity and Access Management (IAM)
 - AWS Trusted Advisor
 - Amazon CloudWatch / AWS CloudTrail
- **Google Cloud**
- **Sonstige Anbieter**
 - Alibaba Cloud
 - Oracle Cloud
- **OwnCloud/NextCloud**

PRÜFUNG direkt im Anschluss:

Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional) deutsch.



Ziele

In dieser dicht gepackten Woche werden alle, für die sichere Nutzung einer Cloud-Infrastruktur, wichtigen Themen behandelt und mögliche Lösungen aufgezeigt. Technische Fragen werden genauso behandelt wie organisatorische Fragen, Risiken und Chancen identifiziert und wichtige Fragen z.B. zur datenschutzkonformen Nutzung diskutiert.

Lernen Sie die Chancen und Risiken der Cloud Nutzung kennen und verstehen Sie die darunterliegende technische Architektur.

Zielgruppe

Das Seminar "Cloud Security Specialist" richtet sich an

- Informationssicherheitsbeauftragte
- Risikomanager
- Cloud-Architekten

in Unternehmen, die Chancen, aber auch Risiken und Gefährdungen der Cloud-Nutzung besser verstehen wollen.

Voraussetzungen

Das Seminar "Cloud Security Specialist" ist sowohl für Einsteiger als auch Fortgeschrittene geeignet. Grundlegende IT-Kenntnisse, Begrifflichkeiten, die in den Kursinhalten verwendet werden, sollten bekannt sein.

- Was sind IP-Adresse, Netzmaske, Default-Gateway
- Was ist eine Firewall, ein VPN-Gateway, ein Webproxy, ein Router, ein Switch
- Was sind Authentifizierung, Autorisierung, Identitätsmanagement
- Was ist Vertraulichkeit, Integrität, Verfügbarkeit
- Was ist Multi-Faktor Authentication
- Was ist eine Sicherheitszone, ein Audit, ein Penetrationstest
- Was ist die DSGVO

NICHT verlangt werde konkrete Kenntnisse als Windows-Administrator oder als Linux-Administrator.



Prüfung/Zertifizierung

CERT CCS Cloud Computing Specialist

Multiple-Choice Prüfung, deutsch

Prüfung zum CBT CERT Zertifikat:

Die Prüfung erfolgt schriftlich als Multiple-Choice Prüfung. Die **CBT CERT Prüfung** wird direkt nach Kursende abgenommen. Sie gilt als bestanden, wenn mindestens 70% der Fragen richtig beantwortet wurden.

Nach Bestehen der Prüfung erhalten Sie ein personenbezogenes **CBT CERT Zertifikat**, das Ihnen die erfolgreiche Kursteilnahme inklusive bestandener Prüfung bestätigt.

Hat ein Teilnehmer die **CBT CERT Prüfung** nicht bestanden, so kann er diese entweder direkt im Anschluss an die erste Prüfung oder während unserer Öffnungszeiten Online Live mit Prüfungsüberwachung (Kamerapflicht, MS-Teams) nach vorheriger schriftlicher Anmeldung (mind. 14 Tage vor Termin) gegen die genannte Prüfungsgebühr wiederholen. Die Prüfung kann höchstens 2-mal wiederholt werden. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Prüfungsversicherung zum CBT CERT:

Haben Sie zum Kurs und zur Prüfungsgebühr unsere Prüfungsversicherung bestellt, berechtigt diese zur **einmaligen kostenfreien Prüfungswiederholung** zu o.g. Bedingungen. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Ohne Prüfungsversicherung zahlen Sie bei Wiederholung die volle Prüfungsgebühr.

Gültigkeit CBT CERT ZERTIFIKAT:

Das **CBT CERT Zertifikat** ist 3 Jahre gültig und muss anschließend durch eine erneute Prüfung bei CBT Training & Consulting GmbH aktualisiert / verlängert werden.
